Schimsa, Rebecca

From: Shihangrs <[redacted]@charter.net>
Sent: Friday, October 26, 2012 6:02 PM
To: Schimsa, Rebecca
Subject: Re: From the Governor's Office re. cyber-attack at DOR

Thanks

Sent from my iPhone

On Oct 26, 2012, at 4:44 PM, "Schimsa, Rebecca" <RebeccaSchimsa@gov.sc.gov> wrote:

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

In regards to the cyber-attack at the Department of Revenue announced this afternoon, we are sending you the following information: (1) the media release from our office (below); (2) the media release from the Department of Revenue (attached); (3) a link to the video of today's press conference; and (4) an invitation to a conference call on Monday morning with Chief Keel, Director Etter, and Inspector General Maley (below).

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

VIDEO OF TODAY'S PRESS CONFERENCE:

The S.C. Department of Revenue announced on October 26, 2012 that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack.

Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel, United States Secret

Service Special Agent in Charge Michael Williams, South Carolina Department of Revenue Director Jim Etter and State Inspector General Patrick Maley today responded to news of the cyber attack with consumer safety solutions during an afternoon press conference.

Video of the press conference is available here: http://www.youtube.com/watch?v=0Dax66JEzVs&
Attached you will find a press kit that includes consumer safety solutions.

Anyone who has filed a South Carolina tax return since 1998 should take the following steps:
1. Call 1-866-578-5422 where you will enroll in a consumer protection service. **The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit http://www.protectmyid.com/scdor. For the US Mail service, you will receive notifications via the US mail.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

Our office has arranged a conference call for members of the General Assembly to be held on Monday, October 29th at 10:00 a.m. with Chief Mark Keel, Director Jim Etter, and Inspector General Pat Maley. The purpose of the conference call is to give you the opportunity to receive information and ask questions about the cyber-attack at the Department of Revenue. There is a limited number of lines available. This call is only intended for you, members of the General Assembly, or a staff member calling in on your behalf.

Call Number: 1-800-670-1742 (No access code is needed.)

Directions:

1. Upon dialing the conference number, each participant will be asked his or her name and then be placed into the conference call.
2. Participants should plan to join the call 5-10 minutes prior to the start of the call.
3. Once the speakers have completed their statements, the call operator will provide instructions for the question and answer portion of the call.
4. All participants will be given the opportunity to ask questions.
5. Questions will be announced in the order that they are received.
6. For operator assistance at any time during the call, please press *0.

-###-

<Media Release from DOR 10.26.2012.pdf>

final drafts - Exec Order and Maley letter

Schimsa, Rebecca

Sent: Thursday, October 25, 2012 6:31 PM

To: Stirling, Bryan; Pitts, Ted; Soura, Christian

Cc: Patel, Swati

Attachments: 2012-10 Reviewing IT Sec~1.docx (25 KB) ; Letter to Maley re EO 2012~1.doc (187 KB)

All – Please see the final drafts of both the Executive Order and the corresponding letter to Maley. With tomorrow morning's press conference now being offsite, I am going to go ahead and have NH sign final versions of these tonight – just in case. Please let us know if you would like changes made.

Thanks.

Rebecca S. Schimsa
Office of Governor Nikki R. Haley
Staff Attorney & Commerce Liaison
O: (803) 734-6068 | C: (803) 429-4561

State of South Carolina
Office of the Governor

NIKKI R. HALEY
GOVERNOR

1205 PENDLETON STREET
COLUMBIA 29201

October 29, 2012

The Honorable Patrick Maley
State Inspector General
110 Centerview Drive, Suite 201
Columbia, South Carolina 29210

Dear Inspector General Maley,

On behalf of state agencies of South Carolina, I request your assistance in addressing a serious issue affecting state government information security.

Throughout state government, our information technology (IT) policy for security procedures and protocols has been largely uncoordinated and outdated exposing our state to greater risks of internal and external cyber-attacks.

I am committed to ensuring that state government minimize the risk of cyber-attacks and protect the personal information of our citizens kept by agencies. Accordingly, today, I signed Executive Order 2012-10 directing the IT officers in my Cabinet agencies to take immediate action to work with the Office of State Inspector General and review and strengthen IT security procedures and protocols.

Pursuant to your authority in Chapter 6 of Title 1 of the South Carolina Code of Laws, I ask that you make recommendations, on a comprehensive and holistic basis, to improve information security policies and procedures in our state agencies.

Sincerely,

Nikki R. Haley

2012-xx

WHEREAS, the State's information technology (IT) policy for governance of IT initiatives throughout state government, including security procedures and protocols, has been largely uncoordinated and outdated exposing the State to greater risks of cyber-attacks on IT infrastructure and records; and

WHEREAS, state government's fragmented approach to IT security makes South Carolina vulnerable to serious cyber and information breaches and requires immediate action to minimize cyber-attacks and protect personal information of our State's citizens; and

WHEREAS, Section 1-6-30 of the South Carolina Code of Laws authorizes the State Inspector General to "coordinate investigations" and "recommend policies and carry out other activities designed to deter, detect, and eradicate fraud, waste, abuse, mismanagement, ..." ; and

WHEREAS, Section 1-6-20(E) states "[u]pon request of the State Inspector General for information or assistance, all agencies are directed to fully cooperate with and furnish the State Inspector General with all documents, reports, answers, records, accounts, papers, and other necessary data and documentary information to perform the mission of the State Inspector General"; and

WHEREAS, the State Inspector General is authorized to recommend policies to address holistic mismanagement of state government's information security policies and procedures and state agencies are required to fully cooperate with the Inspector General to perform his mission.

NOW, THEREFORE, I hereby request the State Inspector General to make recommendations to improve information security policies and procedures in state agencies pursuant to his authority under Chapter 6 of Title 1 of the South Carolina Code of Laws with the following additional guidance:

1. Collaborate with the Division of State Information Technology of the Budget and Control Board to identify weaknesses in the current statewide cyber-security systems and develop a holistic strategy to improve security.
2. Consult with national cyber-security sources including, but not limited to, the Multi-State Information and Sharing Analysis Center.

3. Determine state agencies' current information security staffing and identify designated information security officers (ISOs) at each agency.

4. Improve and increase training of ISOs and all state government employees on information security measures to include cyber-security and records protection.

This Order shall take effect immediately.

GIVEN UNDER MY HAND AND THE GREAT SEAL OF THE STATE OF SOUTH CAROLINA, THIS __ DAY OF OCTOBER 2012.

_____
NIKKI R. HALEY
Governor

ATTEST:

_____
MARK HAMMOND
SECRETARY OF STATE

2012-xx Reviewing IT Security

Patel, Swati

Sent: Thursday, October 25, 2012 10:50 AM

To: Pitts, Ted; Stirling, Bryan; Godfrey, Rob

Cc: Soura, Christian

Attachments: 2012-xx Reviewing IT Sec~1.docx (26 KB)

Here is my final draft pending Christian's input.

2012-10

WHEREAS, the State's information technology (IT) policy for governance of IT initiatives throughout state government, including security procedures and protocols, has been largely uncoordinated and outdated exposing the State to greater risks of internal and external cyber-attacks on IT infrastructure and records; and

WHEREAS, state government's fragmented approach to IT security makes South Carolina vulnerable to serious cyber and information breaches and requires immediate action to minimize cyber-attacks and protect personal information of our State's citizens; and

WHEREAS, Section 1-6-30 of the South Carolina Code of Laws authorizes the State Inspector General to "coordinate investigations" and "recommend policies and carry out other activities designed to deter, detect, and eradicate fraud, waste, abuse, mismanagement . . . "; and

WHEREAS, Section 1-6-20(E) states, "Upon request of the State Inspector General for information or assistance, all agencies are directed to fully cooperate with and furnish the State Inspector General with all documents, reports, answers, records, accounts, papers, and other necessary data and documentary information to perform the mission of the State Inspector General[;]" and

WHEREAS, the State Inspector General is authorized to recommend policies to address holistic mismanagement of state government's information security policies and procedures and state agencies are required to fully cooperate with the State Inspector General to perform his mission.

NOW, THEREFORE, I hereby direct all cabinet agencies to immediately designate an information technology officer to cooperate with the State Inspector General who is authorized to make recommendations to improve information security policies and procedures in state agencies, on a comprehensive and holistic basis,

pursuant to his authority under Chapter 6 of Title 1 of the South Carolina Code of Laws with the following additional guidance:

1. Collaborate with the Division of State Information Technology of the Budget and Control Board to identify weaknesses in current statewide cyber-security systems, to include vulnerabilities to internal and external cyber-attacks, and develop a holistic strategy to improve information security;

2. Consult with national cyber-security sources including, but not limited to, the Multi-State Information and Sharing Analysis Center;

3. Determine state agencies' current information security staffing and their specific duties, and work with agencies to identify designated information security officers (ISOs) and their duties at each agency where appropriate; and

4. Improve and increase training of ISOs and all state government employees on information security measures to include cyber-security and records protection.

This Order shall take effect immediately.

GIVEN UNDER MY HAND AND THE GREAT SEAL OF THE STATE OF SOUTH CAROLINA, THIS 26th DAY OF OCTOBER 2012.

NIKKI R. HALEY
Governor

ATTEST:

MARK HAMMOND
SECRETARY OF STATE